



CHECK POINT TROUBLESHOOTING ADMINISTRATOR (CCTA)



AUDIENCE

This course is designed for security administrators and Check Point resellers who need to manage and monitor issues that may occur within their Security Management environment.

TOPICS



GOALS

Demonstrate and apply understanding of the concepts and skills necessary to troubleshoot issues that may occur when managing the Security Management environment.



PREREQUISITES

Working knowledge of UNIX and/or Windows operating systems. Working knowledge of Networking TCP/IP, CCSA training/certification. Advanced knowledge of Check Point Security products.

TOPICS

Introduction to Troubleshooting Fundamentals

Fundamentals of Traffic Monitoring

SmartConsole and Policy Management Troubleshooting

Identity Awareness Troubleshooting

Access Control Troubleshooting

Troubleshooting Issues with NAT

Understanding Threat Prevention

License and Contract Troubleshooting

OBJECTIVES

- Identify online resources for Check Point security products and solutions.
- Demonstrate understanding of capture packet technologies.
- Demonstrate understanding of Firewall chain modules, Kernel and User Mode, and Kernel and User Space.
- Use Linux and Check Point utilities to review processes and system information.
- Troubleshoot log collection issues and interrupted communications.
- Monitor network activity and traffic flow.
- Demonstrate understanding of Check Point SmartConsole and Policy installation.
- Investigate and troubleshoot issues with Check Point SmartConsole and Policy installation.
- Demonstrate understanding of Check Point Identity Awareness.
- Investigate and troubleshoot issues with Check Point Identity Awareness.
- Demonstrate understanding of Check Point Application Control and URL Filtering.
- Investigate and troubleshoot issues with Check Point Application Control and URL Filtering.
- Demonstrate understanding of Check Point Network Address Translation.
- Investigate and troubleshoot issues with Check Point Network Address Translation.
- Demonstrate understanding of Check Point Threat Prevention.
- Investigate and troubleshoot issues with Check Point Threat Prevention.
- Demonstrate understanding of Check Point licenses and contracts.
- Investigate and troubleshoot Check Point licenses and contracts.

EXERCISES

- Using tcpdump and Wireshark
- Viewing Firewall Chain Modules
- Using Basic Linux and Check Point Commands
- Troubleshooting Logging Communication Issues
- Analyzing Traffic Captures
- Troubleshooting SmartConsole and Using SmartConsole Tools
- Troubleshooting Identity Awareness
- Troubleshooting Application Control and URL Filtering
- Investigating Network Address Translation Issues
- Evaluating Advanced Threat Prevention Products
- Verifying Licenses



CHECK POINT TROUBLESHOOTING EXPERT (CCTE)



AUDIENCE

This course is designed for security experts and Check Point resellers who desire to obtain the necessary knowledge required to perform more advanced troubleshooting skills while managing their security environments.



GOALS

Provide advanced troubleshooting skills to investigate and resolve more complex issues that may occur while managing your Check Point Security environment.



PREREQUISITES

Working knowledge of UNIX and/or Windows operating systems, Working knowledge of Networking, TCP/IP, CCSE training/certification, Advanced knowledge of Check Point Security Products.

TOPICS

- Advanced Troubleshooting Techniques
- Advanced Logs and and Monitoring
- Management Database and Processes
- Advanced Kernel Debugging
- User Mode Troubleshooting
- Advanced Identity Awareness Troubleshooting
- Advanced Access Control
- Site-to-Site VPN Troubleshooting
- Client-to-Site VPN Troubleshooting

OBJECTIVES

- Demonstrate understanding how to use advanced troubleshooting tools and techniques including: Interpreting diagnostic data with CPInfo, Collecting and reading statistical data using CPView, and Advanced troubleshooting risks.
- Describe the use of Logs and SmartEvent in troubleshooting.
- Describe the log indexing system and issues that can occur.
- Discuss methods to troubleshoot log indexing in SmartLog and SmartEvent.
- Explain the databases used in Security Management operations.
- Identify common troubleshooting database issues.
- Discuss Management Processes.
- Demonstrate understanding of advance troubleshooting tools and techniques including: How the kernel handles traffic, How to troubleshoot issues using chain modules, How to use the two main procedures for debugging the Firewall kernel, and How the two main procedures for debugging the Firewall kernel differ.
- Demonstrate understanding of user mode debugging, including collecting and interpreting process debugs.
- Debug user mode processes.
- Discuss advanced Identity awareness troubleshooting.
- Learn to run debugs on Identity Awareness.
- Explain Unified Access Control flow and processes.
- Explain Access Control kernel debugs.
- Describe Access Control process debugs.
- Explain basic and advanced Site-to-Site VPN troubleshooting tools and techniques, including: Packet captures, IKE debugs, and VPN process debugs.
- Explain Client-to-Site VPN troubleshooting tools and techniques, including: Remote access troubleshooting and Mobile access troubleshooting.

EXERCISES

- Collecting and Reading CPInfo
- Collecting and Reading CPView Data
- Troubleshooting SmartLog
- Troubleshooting SmartEvent
- Troubleshooting Database Issues
- Debugging Security Gateway Kernel
- Debugging User Mode Processes
- Debugging Identity Awareness
- Debugging Unified Policy Inspection
- Troubleshooting Site-to-Site VPN
- Debugging Remote Access VPN